Side channel analysis of some hash based MACs:A response to SHA-3 requirements

Gauravaram, Praveen; Okeya, Katsuyuki

Side channel analysis of some hash based MACs: A response to SHA-3 requirements

ICICS 2008

Praveen Gauravaram[1] and Katsuyuki Okeya[2]

Department of Mathematics [1]
Technical University of Denmark (DTU)
Denmark.
Systems Development Laboratory[2]
Hitachi, Ltd
Japan.

Overview of the Presentation

- Research problem
- Hash functions and hash based MACs
- SCA attacks and our model to analyse hash based MACs
- DPA of recently proposed hash based MACs
- Summary and open questions

Research Problem.

Motivation

- Background
  - Cryptanalysis of standard hash functions (MD5 & SHA-1)
  - Generic attacks on the Merkle-Damgård structure
  - Necessity for new hashing methods
  - AHS competition of NIST to augment FIPS 180-2 secure hash standard (SHS)
  - The new SHS will be SHA-3 family.
- Requirement of a hash submission to the AHS competition
  - Support for the FIPS applications (FIPS 198 HMAC)
  - Consideration of side channel attacks (SCA) on the hash based MACs
    1. Resistance to SCA for HMAC configuration
    2. Resistance to SCA for other MAC configurations

Research Problem

- Hypothesis
  - New hash and compression function modes as SHA-3 candidates
  - Compression function modes could be based on block ciphers (PGV)
- SHA-3 requirement
  - Hash modes should define either a HMAC or a dedicated MAC mode
  - Any MAC mode should have protection from the SCA attacks
- Research questions
  - Security of recent hash and compression function modes in the HMAC setting against SCA?
  - Security of recently proposed alternatives to HMAC against SCA?
  - How such an analysis can contribute to the AHS competition?

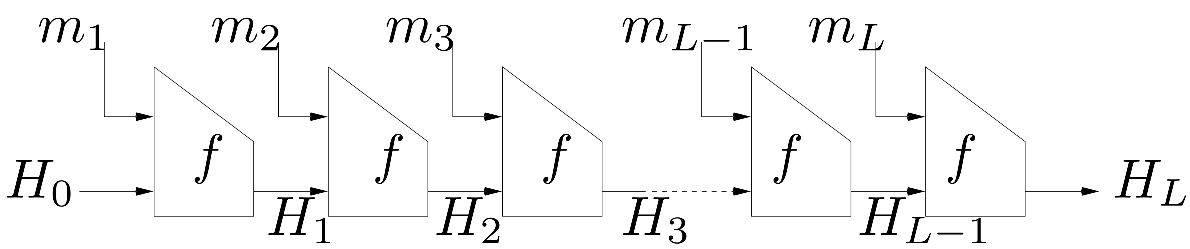
Our approach

- Classify to be analysed MACs into two categories
  - *Type-1:Provably secure MAC alternatives to NMAC/HMAC*
    Examples: BNMAC, KMDP, EMD MAC, Multi-lane NMAC and O-NMAC
  - *Type-2: HMAC/NMAC configuration of the compression and hash modes*
    Examples: MDC2, Grindahl, MAME and Wide-pipe hash
- MAC schemes with no hash analysis
  Examples: BNMAC, O-NMAC
- DPA attack model assumes that the block cipher is DPA resistant

Hash functions and hash based MACs

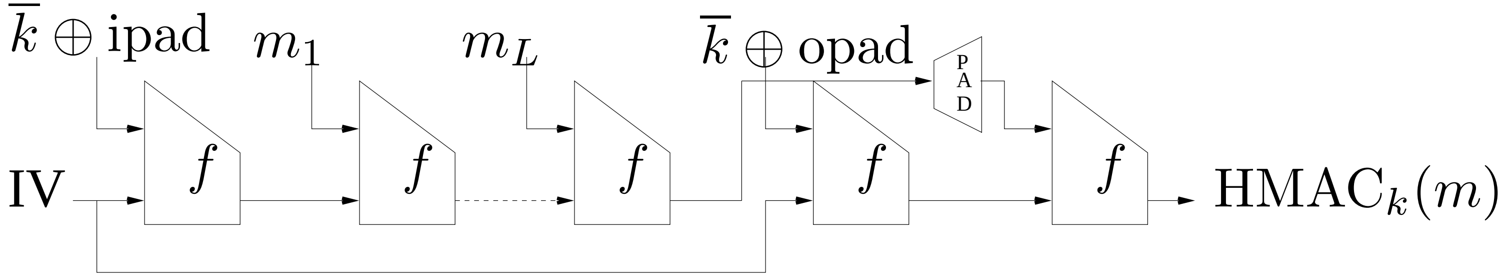
Hash Functions

- $H : \{0,1\}^* \longrightarrow \{0,1\}^n$, $H(M) = Y$
- Merkle-Damgård iterative structure
- Popular hashes: MD4, MD5, SHA-0/1, SHA-224/256 and SHA-384/512



MAC Algorithms

- Verify the integrity and authenticity of the information
- Secure MAC: Hard to find a new (m, $\mathrm{MAC}(m)$) pair even after seeing a few of them
- Attacks include forgery and key-recovery
- Forgeries
  - Universal
  - Selective
  - Existential
- HMAC is FIPS PUB 198 standard

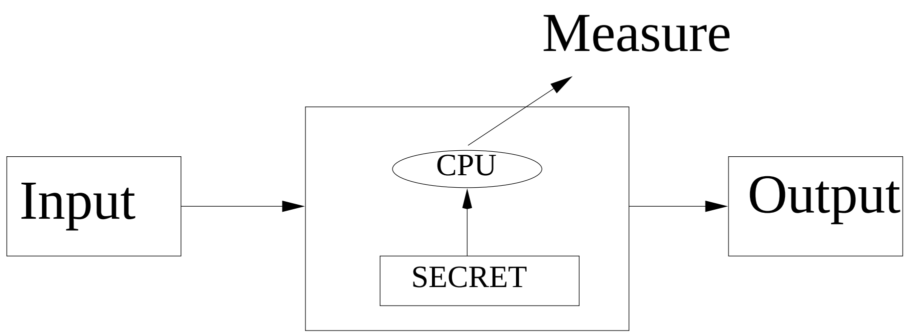


- NMAC is a variant of HMAC.

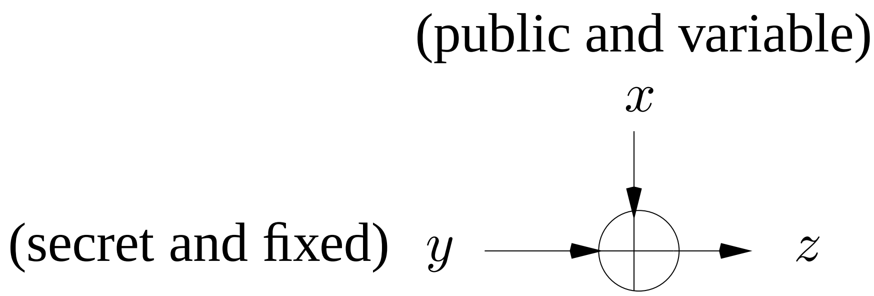
SCA attacks and our model

Side Channel Attacks

- Serious threat to the computing devices that often use secret-key algorithms
- Side channel information is linked with the secret key
- Correlate physical measurements and computing time with the internal state correlated to the secret key
- Reveal secret internal state or the key itself

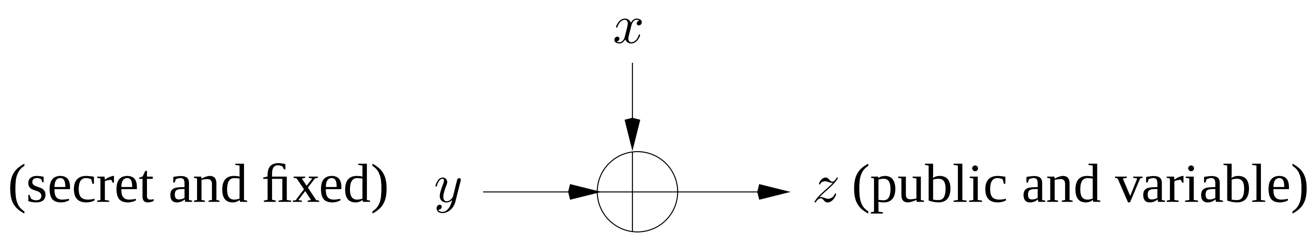


DPA attack model



- DPA attack:
  1. Guess some bit of y
  2. Classify x into two groups.
     (a) Group 1: target bit of $z = 1$
     (b) Group 0: target bit of $z = 0$
  3. Measure the output power signal for each group
  4. Compute average power signal for each group and measure their difference
  5. Use DPA bias signal to verify the guess of y
  6. Repeat (1)-(5) to recover y

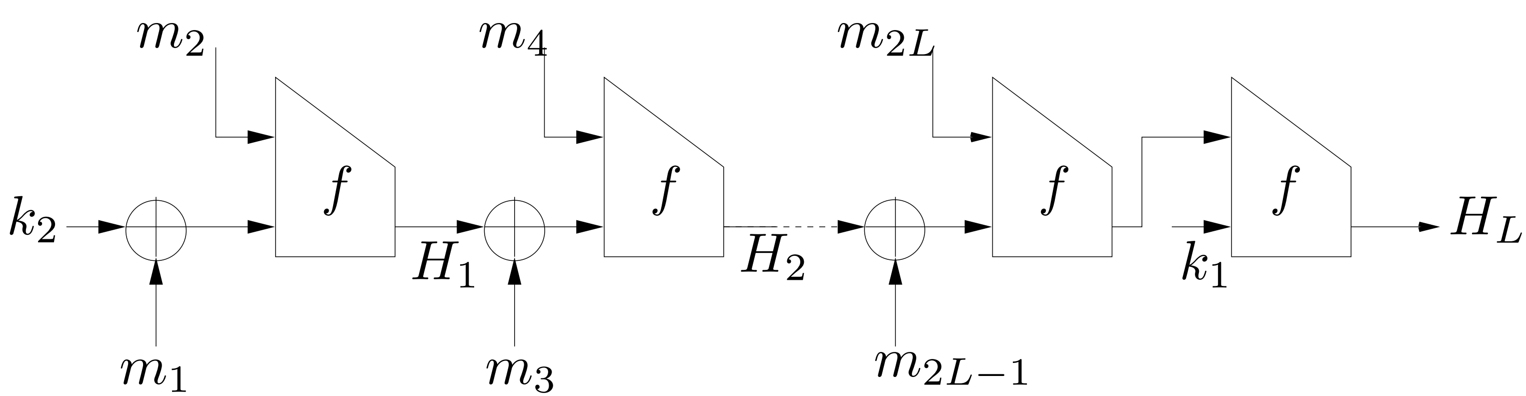
Reverse DPA attack model



- RDPA attack:
  1. Guess some bit of y
  2. Measure the power signal
  3. Retrieve and classify z into two groups
     (a) Group 1: target bit of $x = 1$
     (b) Group 0: target bit of $x = 0$
  4. Compute average power signal for each group and measure their difference
  5. Use DPA bias signal to verify the guess of y
  6. Repeat (1)-(5) to recover y

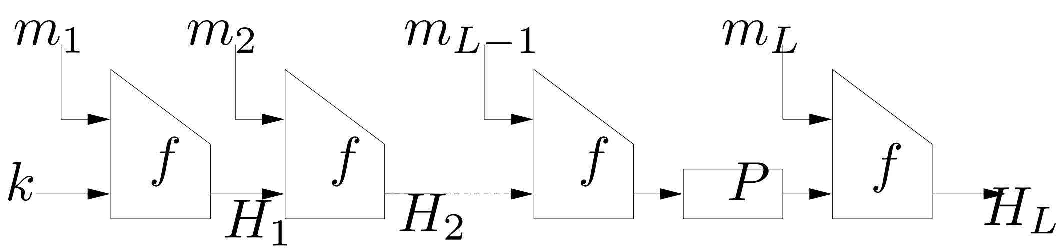
DPA analysis of recently proposed hash based MACs

DPA attack on BNMAC

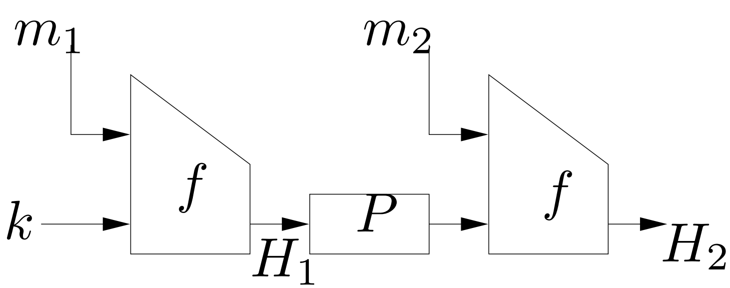


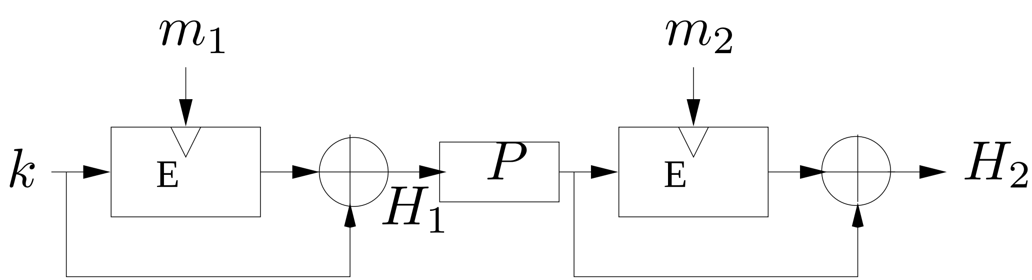
- Mount DPA attack on $H_i \oplus m_{2i+1}$(or $k_2 \oplus m_1$) and recover k_2
- Padding procedure in BNMAC does not depend on the message length
- Recovery of k_1 depends on the architecture of f
- k_2 is enough to forge BNMAC:
    1. Ask BNMAC tag for $m = m_1 \| m_2 \| \ldots \| m_{2L-1} \| m_{2L}$
    2. Set $m_3^* = H_1 \oplus (m_1 \oplus k_2)$ and $m_4^* = m_2$
    3. Set $m^* = m_1 \| m_2 \| m_3^* \| m_4^* \ldots \| m_{2L-1} \| m_{2L}$
    4. $\mathrm{BNMAC}_{k_1,k_2}(m) = \mathrm{BNMAC}_{k_1,k_2}(m^*)$

KMDP using PGV schemes



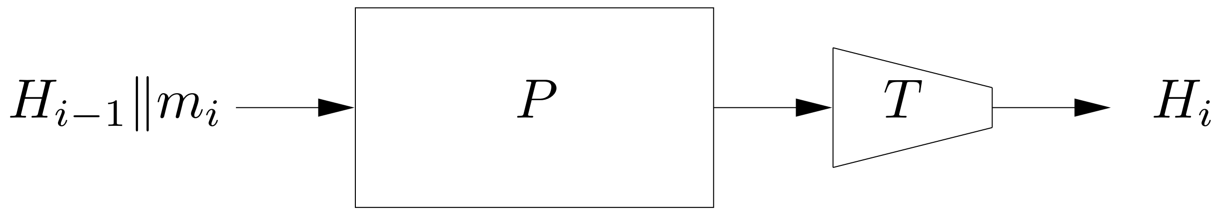
- Security against DPA attacks is almost similar to that of NMAC/HMAC
- RDPA attack on KMDP based on Davies-Meyer:



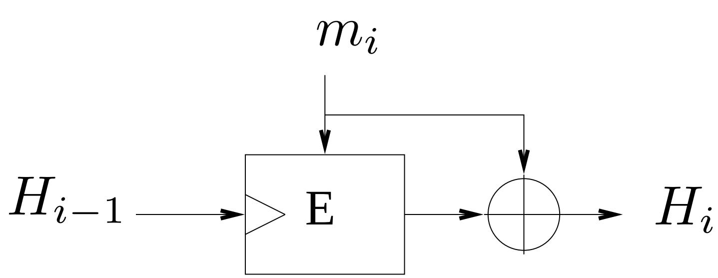


1. Mount RDPA on $P(H_1) \oplus E_{m_2}(P(H_1)) = H_2$ using N^2 of $m_1 \| m_2$ and recover N values of $P(H_1)$ and then H_1
2. Mount RDPA on $k \oplus E_{m_1}(k) = H_1$ using N of H_1 to recover k

Grindahl and MDC2 compression functions



- No target XOR operation when P is ideal
- SCA resistant when P is ideal
- MDC2 which uses Matyas-Meyer-Oseas also does not expose any target XOR operation



Summary of results

MAC function	Matyas-Meyer-Oseas	Miyaguchi-Preneel	Davies-Meyer
BNMAC	PK(EF)	CK(UF)	CK(UF)
EMD	N/A	N/A	PK(NG)
KMDP	NO	NO	CK(UF)
Multi-lane NMAC	N/A	N/A	PK(NG)
O-NMAC	NO	NO	NO
NMAC	NO	NO	PK(NG)

- Wide-pipe hash in the HMAC mode has the same DPA security as HMAC
- MAME compression function in the HMAC mode is DPA resistant

Open questions

Open questions

- How to design a block cipher based multi-property preserving hash construction which is also a SCA resistant when it is instantiated with any of the secure PGV schemes
- Design of a provably secure MAC construction using HAIFA and double-pipe hash invoked with secure PGV schemes and their analysis w.r.t SCA attacks
- What type of alternatives to MD can be plugged into NMAC/HMAC?

Acknowledgments

- Support from the Danish Research Council for Technology and Innovation for the project SHA-3 hash function (`http://www2.mat.dtu.dk/sha3/`)
- Nasour Bagheri (DTU, Denmark)
- Julia Borghoff (DTU, Denmark)
- Bill Burr (NIST, USA)
- Shoichi Hirose (University of Fukui, Japan)
- John Kelsey (NIST, USA)
- Lars Knudsen (DTU, Denmark)
- Gregor Leander (DTU, Denmark)
- Krystian Matusiewicz (DTU, Denmark)
- Søren Thomsen (DTU, Denmark)
- Erik Zenner (DTU, Denmark)